

Ликбез для родителей: как уберечь детей от опасности в интернете.

Поднимая вопросы безопасности детей в интернете, часто говорят о том, что разрешать и запрещать ребенку. Увы, часто родители сами являются причиной бед своих детей, бесконтрольно выставляя на показ их жизнь в соцсетях.

Но давайте по порядку. Здесь доступным языком рассказывается об угрозах, которым подвергаются дети в Сети. Описываются последствия. Приводятся примеры. И конечно, даются практические советы – как защититься, не нарваться и предупредить.

Интернет – это улица

Мир изменился. В Интернете есть почти все развлечения и «развивашки», которые могут понадобиться ребёнку в реальном мире: паззлы, мультфильмы, головоломки, песенки, общение. Дать гаджет в руки чаду для многих эквивалентно покупке тишины и спокойствия. Родитель знает: следующие 30 минут ребенок будет рядом с планшетом или смартфоном.

Вот только бездумно пускать детей в Сеть без каких-либо ограничений точно не стоит. Можно провести аналогию с улицей. Сперва ребёнок гуляет только под вашим присмотром. Затем, со временем, вы начинаете оставлять его одного. При этом объясняете самые важные правила: с незнакомыми не разговаривать, со двора не уходить, на виду быть и т.д. Никому и в голову не придёт высадить трёхлетнего ребёнка посреди города и ждать, что он сам разберётся, как приехать домой.

Но именно так выглядит ситуация, если дать ему гаджет с «неограниченным» интернетом. Молодое поколение должно делать первые шаги в Сети под вашим руководством. И если дочитав до этого места вы думаете, что решили проблему – ведь есть «детский режим», «белые списки» и прочие защитные средства – не спешите. Прежде, чем ограничивать в Интернете ребёнка, давайте ограничим вас.

Как родитель может испортить жизнь детям

Оказалось, что вырастая, дети с удивлением (а некоторые и с ужасом) узнают, что родители годами выкладывают в публичный доступ их фото, личные истории и просто различные аспекты жизни. Созданием онлайн-личности своих детей занимаются не только мамы-блогеры. Этим занимаются множество среднестатистических родителей. Почти у четверти детей цифровая жизнь сегодня начинается с того, что их родители выкладывают фотографию с УЗИ в интернет, как указано в исследовании, проведённом компанией AVG, занимающейся безопасностью в интернете. Также было обнаружено, что у 92% младенцев возрастом до двух лет уже есть своя цифровая личность.

Но даже если вы думаете, что не выкладываете в Сеть «ничего такого» о вашем ребёнке, отдавайте себе отчёт в том, что Интернет всё помнит! Выложив что-либо в Сеть (не обязательно в публичный доступ), вы принимаете риск, что больше не можете контролировать эту информацию. Выложенную фотографию могут «пересохранить», «заскринить» или просто поделиться ссылкой, а сохранит кто-то другой. Где затем всплыт ваша информация, и всплыт ли, неизвестно.

Интернет реально стёр ограничения в общении как в технологическом, так и в экономическом плане. Буквально 30 лет назад наше общение ограничивалось территорией и финансовыми возможностями. Если у вас были деньги, вы могли устанавливать новые контакты либо поехав куда-то, либо позвонив. Существующие ограничения лимитировали не только «позитивные» контакты, но и «негативные». Часто ли вы лет 30 назад встречали в реальном мире троллей, психически нездоровых личностей, шантажистов и прочих злодеев? Интернет дал возможность расширить круг общения не только вам, но и им. И это может стать проблемой.

Самое неприятное, что примеров достаточно, как в «даркнете», так и в «белом» сегменте Сети. Навскидку нашлось с десяток ресурсов, где кто-то собирает фото детей – как они называют, «легальных» фотографий, разбивая снимки по категориям.

Судя по активности, за один месяц, на ресурсе был выставлен 271 пост – мы сами охотно отдаём фото наших детей таким «коллекционерам». «Но как же так? Куда смотрит полиция?! Срочно закрыть!», – говорит вам внутренний голос. Если бы все было так просто: «технически» такие ресурсы не нарушают закон. Подобные сайты периодически прекращают своё существование. И открываются вновь.

Так что же делать? Взвешивайте риски,уважаемые родители, когда решите поделиться с миром очередной личной историей, фотографией и т.д. И тем более – отметить геопозицию домашней фотографии.

Опасности, которые ребёнок находит сам

Настало время поговорить об угрозах и последствиях. Самая плохая мысль, которой вы можете придерживаться – «*Это не про меня*». Это не про вас и вашего ребёнка ровно до тех пор, пока это не случится. Но тогда уже может быть поздно. Например:

«Кривое зеркало» социальных сетей

Пользователи социальных сетей культивируют приукрашенные образы людей. Стоит зайти в Instagram, Facebook, etc. и убедиться, что на каждом шагу видно успешных путешественников, бизнесменов, бьюти-блогеров и прочих крайне крутых персонажей. Если ребёнку не объяснить правила игры, он будет искренне верить, что так на самом деле и есть.

А помимо успешности в соцсетях красной лентой проходит ещё одна опасная мысль: *ты ЛЕГКО можешь быть таким*. Ну что сложного снять «крутой» видос? Особенно когда даже государство видит в этом пользу и выделяет существенные средства на школу TikTok'a. Честно, не знаю, чему конкретно могут научить в такой школе. Но вряд ли это будут курсы по сценарному делу, актёрскому мастерству, операторскому искусству и режиссуре. Скорее скажут что-то вроде: «Снимай крэйзи, снимай дичь! Крэйзи и дичь хорошо вирусится».

Как один из итогов, свежий пример: две подруги (16 и 17 лет) забрались на крышу пятиэтажки, чтобы сделать селфи. Стоя на краю, девушки делали совместные фото. В какой-то момент 16-летка поскользнулась и упала с крыши.

Проблема в том, что желание «быть популярным» может превратиться в желание «быть популярным любой ценой». А вот это уже вряд ли закончится хорошо.

Буллинг, шантаж, доведение до суицида «Травить» могут за что угодно. Вообще никакой систематизации здесь нет. Буллинг усугубляется соцсетями и мессенджерами, когда ребёнок после занятий не получает паузу для психики, потому что травля из мира реального перетекает в Интернет. Попробуйте сами быть под жёстким прессингом почти всё время, что не спите. Долго ли выдержите? А теперь представьте, каково может быть ребёнку, который по какой-то причине стесняется или не хочет спросить совета родителей.

Любопытство. На каком-то этапе взросления всё, что опасно автоматически может причисляться к крутым. Когда-то круто было иметь «Поваренную книгу Анархиста» или «Лики смерти». А вот не так давно «модно» было проверить свои нервы в игре «Синий кит». «Разбуди меня в 4:20» и вот это вот всё. Помните? Дети из любопытства сами могут вляпаться во что-то, а потом из-за впечатлительности и страха не рассказать о наступивших проблемах.

Неправильно оценённые риски распространения отправленной информации. Незнание того, как работают технологии, приводит к неправильной оценке рисков. Например, пользователи приложения Whisper видимо искренне верили, что их секреты анонимны. Однако в 2020 году оказалось, что компания годами непреднамеренно раскрывала такие данные пользователей, как возраст, этническую принадлежность, место жительства, местоположение, псевдоним в приложении и членство в любых группах. Объясняйте детям и помните сами, что наличие в Сети какой-то «чувствительной информации» может использоваться для шантажа, мошенничества и просто травли.

Как защитить ребёнка

Если вы думаете, что есть «серебряная пуля», то наступило время разочарований. Универсального метода нет. Но есть несколько советов, которые работают. Их расположим не по мере эффективности, а по мере взросления ребёнка:

Детские режимы

Начинается всё с них. Это та пора, когда чадо настолько мало, что не имеет собственного личного гаджета. Ребёнку время от времени «перепадает» родительский девайс, на котором включается «Детский режим». Это специальная программа, из которой он не может сам выйти. Родитель может настраивать, к каким приложениям у пользователя будет доступ, сколько времени можно играть и т.д.

В правильном возрасте и при правильной настройке со стороны родителей детские режимы довольно эффективны. Но есть нюансы. Если вы просто дадите ребёнку доступ к браузеру, то толку от «детского режима» никакого. Хорошо, тогда дадим доступ к «детскому браузеру». Или «детскому ютубу» (такой тоже есть). Подобные приложения «хорошие» за счёт модерации контента. То есть где-то там в какой-то компании сидит цензор и решает, что можно смотреть детям, а что нет. Надеюсь, вам понятно, что там, где есть человек, есть место и человеческим ошибкам. Поэтому на детский режим надейтесь, но совсем без контроля, чем занимается ребенок в сети – не оставляйте.

Белые списки, детский Интернет

Много компаний продают услугу со словом «детский». Принцип аналогичен белым спискам: можно ходить только на те сайты и запускать только те программы, которые разрешены. Разрешил либо сам родитель, либо «цензор» со стороны компании. Подход вполне рабочий. Ребёнок получает доступ не просто к «белому», а к «самому белому» Интернету.

Но проблема белых списков точно такая же, как и у «детских режимов». Ребёнок может случайно либо намеренно прорваться в «настоящую» Сеть. Способов уйма и дети освоят их гораздо быстрее, чем вы.

Помните – дети любопытны, и, если им что-то интересно, они это найдут. Если родитель не включил «безопасный поиск», то даже названий сайтов знать не надо. Не находит поисковик – ищем в соцсетях. А можно начать осваивать VPN и proxy. А если ребенок видит, что вы запрещаете этим интересоваться, значит это точно интересно. Эффект одной Барбары, знаете ли. А какая часто реакция у родителей на это?

Никакого Интернета!

Реакция естественная, но тупиковая. Даже не знаю, что тут ещё написать. С сегодняшним уровнем доступности и проникновения в жизнь технологий, не представляю, как можно эффективно «отключить» ребенка от Сети. Компьютеры есть в школе, смартфоны есть у друзей.

Слежка

А вот это работает. Ровно до тех пор, пока вы себя не раскроете, либо сам ребёнок не догадается о контроле. Например, можно посматривать на историю в браузере. Или установить соответствующие программы. Или подарить специальные [«детские часы»](#). Рынок предлагает уйму способов на любой вкус. Но готовы ли вы к последствиям? В тот момент, когда слежка вскроется, вы рискуете потерять доверие ребёнка навсегда. Поэтому либо имейте в запасе план по улаживанию конфликта, либо будьте настолько искусны, чтобы не попасться.

Просвещение и «мягкая сила»

Это самый эффективный способ. Он же и самый сложный. Важно соблюдать баланс. Можно запретить ребенку все – и нарваться на активное противодействие. Можно быть максимально открытым, но в определённом возрасте подростку может быть просто неудобно обсуждать эти темы с вами.

И здесь на сцену выходит «мягкая сила». Когда вы обсуждаете с ребенком – почему можно, почему нельзя, чем грозит бесконтрольность. А также даете ему самому разобраться в вопросах, которые он не хочет обсуждать с вами. У нас не так много дальних проектов по безопасности, рассчитанных на детей, но примеры есть: kids.kaspersky.ru, где можно выбрать контент для детей, подростков и взрослых; или www.kaspersky.ru/about/press-releases/2017_kaspersky-fixiki – где о безопасности

ребенку расскажут Фиксики.

В общем, не стесняйтесь учиться поведению в Сети сами, если что-то не знаете. Разговаривайте со своими детьми. Молчание, хоть и золото, но не в этом случае.

Источник: <https://habr.com/ru/company/searchinform/blog/504434/>